UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/932,408	08/18/2001	Russell Dickerson	35997-217836	4316

26694   7590   03/29/2006

VENABLE LLP
P.O. BOX 34385
WASHINGTON, DC 20045-9998

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2006*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-16 and 19-24* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-9, 11-16 and 19-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the Appeal Brief filed on March 17 2006. Claims 1 –

24 were originally received for consideration as currently pending in the application.

Response to Arguments

In view of the Appeal Brief filed on March 17 2006, PROSECUTION IS HEREBY

REOPENED *because the previous Nasu reference does not explicitly teach a system*

that obstructs access by an in-circuit emulator to the secure area, when an in-circuit

emulator requests access to the secure area. A new ground of rejection, with Tabe

reference U.S. Patent 6.622,184, is set forth below to enter the Amendment After-Final

(1) incorporated dependent claim 10 into independent claim 1 and dependent claims 17

and 18 into independent claim 13 and (2) claims 10, 17 and 18 were canceled.

To avoid abandonment of the application, appellant must exercise one of the

following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a

supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or

1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that

forms the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1.   Claims 1 – 9, 11 and 13 – 16, 19 – 22 are rejected under 35 U.S.C. 102(e) as

anticipated by Tabe et al. (U.S. Patent 6.622,184).

As per claim 1, Tabe teaches a method for obstructing access to a secure area

of a semiconductor device comprising:

connecting an in-circuit emulator to the semiconductor device (Tabe: Column 1

Line 20 – 27 and Figure 3);

generating a command from the in-circuit emulator (ICE) to the semiconductor

device, wherein the command requests access to the secure area of the semiconductor

(Tabe: Column 2 Line 9 – 11, Column 1 Line 32 – 39 and Column 3 Line 66 – 67: the

protected access to built-in ROM at power up by the ICE is considered as the access to

the "secure area");

providing a control signal indicating that the semiconductor device has entered a

secure mode (Tabe: Column 3 Line 64 – 67 and Figure 3 Element 3: the security

enabling signal as taught by Tabe is interpreted as the control signal); and

obstructing access to the secure area utilizing the control signal (Tabe: Column 2

Line 9 – 11, Column 1 Line 32 – 39 and Column 3 Line 66 – 67).

As per claim 13, Tabe teaches a system for obstructing access to a secure area

of a semiconductor device comprising:

a port for an in-circuit emulator (Tabe: Figure 3 Element 1 / Element 2);

a first circuit for generating a control signal (Tabe: Column 2 Line 9 – 11 and

Column 3 Line 66 – 67: a debug control signal is generated by the on-chip debug ICE to

enter the ICE debug mode at power up); and

a second circuit for obstructing access to the secure area connected to the

control signal (Tabe: Column 3 Line 56 – 67 and Figure 3 Element 3: the security circuit

as taught by Tabe is considered as the second circuit), wherein the control signal is

utilized by the second circuit to obstruct access to the secure area when a mode

indicated by the control signal is a secure mode (Tabe: Column 2 Line 9 – 11, Column 1

Line 32 – 39 and Column 3 Line 66 – 67), and wherein the semiconductor device enters

the secure mode when the in-circuit emulator is connected to the port (Tabe: Column 2

Line 9 – 11, Column 1 Line 32 – 39 and Column 56 – 67: the protected access to built-in

ROM at power up by the ICE is considered as the access to the "secure area" and

thereby enters the secure mode).

As per claim 2 and 14, Tabe teaches obstructing access to the secure area comprises gating another signal with the control signal (Tabe: Figure 3 Element 8 / Element 9).

As per claim 3 and 4, Tabe teaches obstructing access to the secure area comprises is selecting a multiplexer channel with the control signal (Tabe: Figure 3 Element 8 / Element 9: the control signal is considered as the Security Enabling Signal).

As per claim 5, Tabe teaches the secure area is used in connection with data encryption (Tabe: Column 7 Line 7 – 10).

As per claim 6, Tabe teaches providing a control signal further comprises decoding a plurality of signals to generate the control signal (Tabe: Figure 3 Element 3).

As per claim 7, 8 and 9, Tabe teaches the control signal transitions from a first logic state to a second logic state when the semiconductor device enters the secure mode (Tabe: Figure 3 Element 3).

As per claim 11, Tabe teaches the semiconductor device enters the secure mode when the in-circuit emulator is connected to the semiconductor device (Tabe: Column 2 Line 9 – 11 and Column 3 Line 66 – 67: a debug control signal is generated by the on-chip debug ICE to enter the ICE debug mode at power up).

As per claim 15, Tabe teaches the logic gate is an AND gate having a first input connected to the first circuit such that the first input responds to the control signal; a second input connected to a circuit supplying output data; and an output connected to a port of the semiconductor device (Tabe: Figure 8 Element 8 & 9).

As per claim 16, Tabe teaches the second circuit is a multiplexer (Tabe: Figure 3 Element 4).

As per claim 19, Tabe teaches the secure area comprises memory (Tabe: Column 2 Line 9 – 11, Column 1 Line 32 – 39: the protected access to built-in ROM at power up by the ICE is considered as the access to the "secure area").

As per claim 20, Tabe teaches the semiconductor device is an application specific integrated circuit (Tabe: Figure 1 Element 101).

As per claim 21, Tabe teaches the first circuit is a microprocessor core (Tabe: Figure 3 Element 1).

As per claim 22, Tabe teaches the first circuit is a decoder (Tabe: Figure 3 Element 3).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 23 – 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Tabe et al. (U.S. Patent 6.622,184), in view of Applicant Admitted Prior-art (Publication

Number: US 2003/0212897 A1), hereinafter referred to as AAP.

As per claim 24, Tabe teaches a system for obstructing access to a secure area

of a semiconductor device comprising:

a microprocessor core (Tabe: Figure 3 Element 1);

a decoder connected to an output of the microprocessor core (Tabe: Figure 3

Element 3 / Element 9: the OR gate has two inputs (a) data output line (b) the Security

Enabling Signal derived by the decoder of security circuit (Element 3)).;

a control line connected to an output of the decoder (Tabe: Figure 3 Element 8 &

9 / Element 3: the control line is generated from the Security Enabling Signal);

a circuit for supplying output data decoder (Tabe: Figure 3 Element 9);

a data output line connected to an output of the circuit for supplying output data

(Tabe: Figure 3 Element 9); and

an AND gate having a first input connected to the control line, a second input

connected to the data output line (Tabe: Figure 3 Element 8 / Element 9: the combined

END gate (Element 8) with the OR gate (Element 9) is inherently equivalent to a AND

gate with three inputs – i.e. (1) control line (as Security Enabling Signal), (2) data output

line (as the data output from ICE) and (3) the control signal. This is because the

Security Enabling Signal, as taught by Tabe in Figure 3, is connected simultaneously to

not only AND gate but also OR gate and thereby these two gates is indeed functioned

as <u>one single entity of AND gate</u> because, for example, a HIGH level of Security

Enabling Signal would not only disable the AND gate but also unconditionally raised the

data output line to HIGH via OR gate), and an output connected to an input of a buffer

(AAP: Figure 3A / Element 48);

and a port implemented in the semiconductor device for connecting to an in-

circuit emulator (Tabe: Figure 3 Element 1 & 2), wherein a line on the port is also

connected to an output of the buffer (AAP: Figure 3A Element 30: TDO line – i.e. the

Test Data Out), wherein when the in-circuit emulator requests access to the secure area

(Tabe: Column 2 Line 9 – 11, Column 1 Line 32 – 39: the protected access to built-in

ROM at power up by the ICE is considered as the access to the "secure area"), the

microprocessor core generates microprocessor signals for decoding by the decoder

(Tabe: Column 3 Line 56 – 67 and Figure 3 Element 3 / Element 9), and wherein the

decoder decodes the microprocessor signals and generates a control signal on the

control line connected to the first input of the AND gate (Tabe: Figure 3 Element 3 & 8),

and wherein the AND gate outputs an obstructing signal to obstruct access by the in-

circuit emulator to the secure area (Tabe: Figure 3 Element 8 / Element 9).

As per claim 23, Tabe teaches the output is buffered before connecting to the

port (AAP: Figure 3A Element 48).

3.   Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tabe et

al. (U.S. Patent 6.622,184), in view of Applicant Admitted Prior-art (Publication Number:

US 2003/0212897 A1), hereinafter referred to as AAP, and in view of Boyce (U.S.

Patent 4,796,258).

As per claim 12, Tabe does not teach the command is a software interrupt.

Boyce teaches the command is a software interrupt (Boyce: see for example,

Column 3 Line 61 – 68: Examiner notes Boyee teaches a microprocessor debug tool

that has a ROM emulator (i.e. equivalent to a ICE tool) with a protected monitor memory

portion for command fragments specified by the user to be executed upon receipt of a

software interrupt on detection of a user specified event (Boyee: Column 3 Line 61 – 68)

and the result of the command execution is detected by a word recognizer to interface

with the user (Boyee: Column 3 Line 68 – Column 4 Line 2). Examiner notes an ICE

command can thus be considered as associated with software interrupt and is executed

as user specified. Therefore, Boyce teaches a software interrupt is generated from a

microprocessor debug tool which has an emulator upon detection of a user specified

event including a user command).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Boyce within the system of Tabe

because Boyce teaches providing a microprocessor debug tool which can effectively

monitor the system operation (Boyce: see for example, Column 1 Line 44 – 47).

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Longbit Chai whose telephone number is 571-272-3788.

The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

CHRISTOPHER REVAK
PRIMARY EXAMINER

3/26/06